UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/955,924	09/19/2001	Christian Huitema	212515	9394

22971 7590 05/10/2005

MICROSOFT CORPORATION
MICROSOFT PATENT GROUP DOCKETING DEPARTMENT
ONE MICROSOFT WAY
BUILDING 109
REDMOND, WA 98052-6399

EXAMINER	
CHAI, LONGBIT	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 05/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/955,924	HUITEMA ET AL.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 March 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 September 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1 – 25 have been presented for examination. Claim 1 has been canceled; claims 2 – 22 have been amended in an amendment filed 3/8/2005.

Response to Arguments

2. Applicant's arguments filed on 3/8/2005 with respect to instant claims have been fully considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 2, 8, 9, 22 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Turnbull (Patent Number: 6092201), in view of Aoki (Patent Number: 6748530).

As per claim 2, Turnbull teaches a method of inviting and joining a peer to a secure peer-to-peer group (Turnbull, Abstract Line 1 – 9) comprising the steps of:

obtaining a public key of a peer; and forming, by a first member of the group, a group membership certificate containing the peer's public key (Turnbull, Figure 1 Element 34);

sending the group membership certificate to the peer to invite the peer to join the group, the group membership certificate allowing the peer to join the group through a second member other than the first member (Turnbull, Column 5 Line 57 – Column 6 Line 6 and Column 6 Line 20 – 23: The invitation of the user 2 by the user 1 to join the group is interpreted based on the situation that the originating user 1 would also be required to be authenticated by the invited user 2 via validating the originating user's signature).

Turnbull does not teach signing with a group private key of a group public / private key pair.

Aoki teaches signing with a group private key of a group public / private key pair (Aoki: Figure 3 and Column 18 Line 38 – 39).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Aoki within the system of Turnbull because Aoki teaches providing a simplified certification apparatus and method that can be performed uniformly and fairly within its own group without necessitating the external 3rd party such as CA (Certification Authority) (Aoki: see for example, Column 19 Line 7 – 13).

As per claim 8 and 9, the claim limitations are met as the same reasons set forth in the paragraph above regarding to claim 2 – such as $((P_{U1})\ K_G)$ with the exception of the feature forming a group membership certificate having a structure $(((P_{U1})\ K_G)\ K_{U2})$. However, Turnbull further teaches forming a group membership certificate having a structure $(((P_{U1})\ K_G)\ K_{U2})$ (Turnbull: Column 6 Line 20 – 23: the originating user 2 (i.e. the issuer) would also be required to be authenticated by the invited user 1 via validating the originating user's signature (i.e. using the additional the issuer's signature which is signed with K_{U2} in addition t o $((P_{U1})\ K_G)$).

As per claim 22 and 23, Turnbull as modified further teaches computer-readable medium having computer-executable instructions (Turnbull: see for example, Figure 2).

4. Claims 13 – 15, 17, 18, 20, 21, 24 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Turnbull (Patent Number: 6092201), in view of Langford (Patent Number: 6266420).

As per claim 13, Turnbull teaches a method of securely joining a peer-to-peer group by a peer having a public and a private key, comprising the steps of:

receiving a group invitation from a first member containing an invitation certificate having a group ID provided therein (Turnbull, Column 5 Line 57 – Column 6 Line 6 and Column 6 Line 20 – 23: (a) The issuer (or the 1st member) first creates the shared list (i.e. functional group ID) and certificates, (b) The invitation of the user 2 by the user 1 to

join the group is interpreted based on the situation that the originating user 1 would also be required to be authenticated by the invited user 2 via validating the originating user's signature).

resolving the group ID to find a third member of the group different from the first member (Turnbull, Column 7 Line 2 – 12: (a) the shared list is equivalent to a functional group ID (b) another user in the group other than the issuer / creator / owner can also be authorized to modify the shared list and provide the modified list to other users via the same process as the original issuer);

sending a connect message to the member containing the invitation certificate signed with the private key (Turnbull, Column 6 Line 20 – 23: The invitation of the user 2 by the user 1 to join the group considered as the "CONNECT" message is interpreted based on the situation that the originating user 1 would also be required to be authenticated by the invited user 2 via validating the originating user's signature).

receiving an accept message from the member containing a group membership certificate signed by a private key of the member (Turnbull, Column 6 Line 20 – 23 and Column 7 Line 28 – 29: The response message associated with the invitation of the user 2 by the user 1 to join the group is considered as the "ACCEPT" message after validating the originating user's signature).

Turnbull does not teach receiving a group shared key to enable decryption of group traffic.

Langford teaches receiving a group shared key to enable decryption of group traffic (Langford: Column 2 Line 49 – 51: group decryption key to decrypt the group traffic).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Langford within the system of Turnbull because Langford teaches providing an effective secure group communication that substantially reduces the data overhead accompanying each secure message in comparison using the security credentials of each of the member (Langford: see for example, Column 2 Line 57 – 60).

As per claim 14, 17, 18 and 20, the claim limitations do not further teach over claim 13. Therefore, see the same rationale set forth above in rejecting claim 13.

As per claim 15, Turnbull as modified further teaches resolving the group ID to find a second member of the group to which to connect when the step of authenticating the group membership certificate signed by the private key of the third member fails (Turnbull: see for example, Column 5 Line 57 – Column 6 Line 27 and Column 7 Line 1 -- 5: (a) the shared list = functional group ID, and (b) the end-user 14 (the issuer) and the authorized modifier needs to continue to complete the certificate validation through out the entire functional group).

As per claim 21, Turnbull as modified further teaches determining if the group membership certificate is listed in a group certificate revocation list (GCRL); when the group membership certificate is listed in the GCRL, determining if a date of revocation is before a date of issuance of the invitation certificate; and when the date of revocation is after the date of issuance, issuing a new group certificate to the peer (Turnbull: Column 8 Line 16 – 36).

As per claim 24 and 25, Turnbull as modified further teaches computer-readable medium having computer-executable instructions (Turnbull: see for example, Figure 2).

5. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Turnbull (Patent Number: 6092201), in view of Aoki (Patent Number: 6748530), and in view of Langford (Patent Number: 6266420).

As per claim 3, Turnbull as modified does not teach generating a group shared key to be used to encrypt group traffic. However, Langford teaches generating a group shared key to be used to encrypt group traffic (Langford: Column 2 Line 49 – 51: group decryption key to decrypt the group traffic).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Langford within the system of Turnbull as modified because Langford teaches providing an effective secure group communication that substantially reduces the data overhead accompanying each

secure message in comparison using the security credentials of each of the member (Langford: see for example, Column 2 Line 57 – 60).

6. Claims 5, 7, 10 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Turnbull (Patent Number: 6092201), in view of Aoki (Patent Number: 6748530), in view of Langford (Patent Number: 6266420).

As per claim 5 and 10, the additional claim limitations to claim 2 and 8 respectively are met as the same reasons set forth in claim 13. See also the same rationale to combine Langford with Turnbull in claim 13.

As per claim 7 and 12, Turnbull further teaches the specific details of the group certificate revocation lists such as determining if the group membership certificate is listed in a group certificate revocation list (GCRL); determining if any certificates in a chain of group membership certificates is listed in the GCRL; when any certificates in the chain is listed in the GCRL, determining if a date of revocation of the certificate in the chain is before a date of issue of the group membership certificate; and when the date of revocation is after the date of issue, issuing a second group membership certificate to the peer (Turnbull: see for example, Column 5 Line 57 – 67, Column 6 Line 2 – 4 and Column 8 Line 20 – 24).

7. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Turnbull (Patent Number: 6092201), in view of Aoki (Patent Number: 6748530), and in view of Aucsmith (Patent Number: 5712914).

As per claim 4, Turnbull as modified further teaches certificate comprises the step of forming a group membership certificate having a structure [Version, ID, Peer ID, Serial Number, Validity, Algorithms, P_{ID}, Pissuer] Kissuer (Turnbull: Column 5 Line 55 -- 27).

Turnbull as modified does not disclose explicitly certificate Version ID, Serial Number, Validity and Algorithms.

Aucsmith teaches certificate Version ID, Serial Number, Validity and Algorithms (Aucsmith: see for example, Column 5 Line 1 – 39).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Aucsmith within the system of Turnbull as modified because Aucsmith teaches the digital certificate conforming to recommendation X.509 for authentication (Aucsmith: see for example, Column 1 Line 10 – 11).

8. Claims 16 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Turnbull (Patent Number: 6092201), in view of Langford (Patent Number: 6266420), and in view of Bolosky (Publication Number: 2002/0194484).

As per claim 16 and 19, Turnbull as modified further teaches verifying that a signature of the certificate is valid; verifying that the certificate has not expired (Turnbull: Column 8 Line 16 – 36);

Turnbull as modified does not teach verifying that the hash of a public key of the peer matches a peer identification of the peer.

Bolosky teaches verifying that a signature of the certificate is valid; verifying that the certificate has not expired; verifying that the hash of a public key of the peer matches a peer identification of the peer (Bolosky: Paragraph [0093] Line 7 – 9).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Bolosky within the system of Turnbull as modified because Bolosky teaches an effective identity-base user security validation mechanism (Bolosky: see for example, Paragraph [0093] Line 7 – 9).

9. Claims 6 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Turnbull (Patent Number: 6092201), in view of Aoki (Patent Number: 6748530), in view of Langford (Patent Number: 6266420), and in view of Bolosky (Publication Number: 2002/0194484).

As per claim 6 and 11, the additional claim limitations to claim 5 and 10 respectively are met as the same reasons set forth in the paragraph above regarding to claim 16. See also the same rationale of combination in claim 16.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100